# Aspects to consider within information security during procurement and use of cloud services

Version: 1.00
Release date: 19-Apr-2013

## Preface

This document is partly based on the authors' previous work [i] made under the Creative Common Share Alike 3.0. If using this document, please reference it properly. The objective with this document is to provide guidance on information security aspects to organizations looking into procurement of cloud services, as well as to organizations already using cloud services. Further, aspects of cloud computing pertaining to compliance frameworks are addressed.

Finally, if you have any ideas for improvement – please do not hesitate to e-mail the contact person for the last version of the document listed below.

## Version history

| Version | Contributors | Approved |
|---|---|---|
| 1.0, first version | **Project leaders/Editors**: John Lindström/Dan Harnesk (LTU)<br><br>**Contributors**: Eva Ekelund, Karl-Mårten Karlsson (Actea Consulting AB), Lars G Magnusson, Lars Perhard (W&P Advokatbyrå KB), Caroline Olstedt Carlström (Klarna AB), Magnus Eklöf, Magnus Lindkvist (Microsoft Sverige AB), Tommy Ståhl, Ulf Berglund (U&I Security AB)<br><br>**Primary contact**: john.lindstrom@ltu.se | 19-Apr-2013 |
| | | |
| | | |

## Contents



## Word list and abbreviations used

| | |
|---|---|
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SECaaS | Security as a Service |
| XaaS | X as a service – used as a collective term to denote "anything" or "everything" as a service |
| CIO | Chief Information Officer – corresponds to a senior management role responsible for IT- and information issues within an organization |
| CISO | Chief Information Security Officer – corresponds to a senior management role responsible for information security issues within an organization |
| Security<br>Information security | When the term "security" or "information security" is used, it encompasses security for IT, information systems and information |

## Before you read this document…please read:

This document has been written for use mainly within Sweden, and although most of the aspects discussed are of a general nature, readers should have this fact in mind while reading.

These guidelines should not be construed as technical or legal advice on any specific facts or circumstances. The content is not exhaustive and is intended for limited general informational purposes only. The authors make no representations as to accuracy, completeness, actuality, suitability, or validity of any information and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis with no warranties, and confers no rights. Readers should consult appropriate technical, accounting or legal consultants concerning any specific question or the relevance of the subjects discussed herein to particular factual circumstances.

# 1. Introduction

This document concerns aspects of information security regarding cloud services. These services are often referred to as SaaS, IaaS and PaaS and can of course be combined, or only partly be used, together with an organization's private IT environment. Recent abbreviations introduced are for instance SECaaS and XaaS. As the interest for cloud services start to gain momentum among stakeholders in an organization, and a procurement process is about to start (or if cloud service already has been procured), there are two questions to consider:

- **What is the problem and challenge with security in the cloud compared to methods used previously?** The problem and challenge involve a number of issues, e.g. it is partly new, that competences and personnel not existing in all organizations are required. The sourcing of personnel and specific competences may need to be examined. Many organizations will also probably need to make changes in their own security and risk management processes, update the legal/regulatory and compliance frameworks used, because there will not be the same transparency and possibilities to investigate, impact or follow up on issues. Many organizations are not familiar with procuring cloud services and the various legal issues which need to be considered.

- **What security problems/areas and related legal and compliance issues need an organization consider?** There is no exact template, as all organizations differ in their business processes. One example is if personal data is stored, processed or communicated within a cloud service, it may require additional actions regarding, e.g., clarification of responsibilities, agreements for export of personal data, and appointing a Personal Data Officer. However, this document comprises a number of problems and areas which we consider are of importance. Any organization should firstly consider what and where there can be problems before this document is used, not become too influenced by it and overlook important factors when the contents in this document are used and "ticked off".

Most organizations have a number of requirements regarding security (regulations, laws or business requirements), and these usually differ depending on whether the organization is a small business, a public corporation, a public authority/government agency, or municipality. In most cases, the top management of an organization has a responsibility to investigate risks related to IT, as well as to take action to mitigate possible risks in a responsible manner. A hinder related to cloud services is that an organization, in most cases, does not have the same possibilities to control, impact or influence, and that an increased transparency is required from providers (see [1, 3, 7]). There is a need to build trust in between the parties. From a legal standpoint, work tasks with related responsibility to maintain the levels of security can be, to a certain degree, delegated to providers by a contractual agreement. For example, regarding a public corporation, its board and president (top management) are always ultimately responsible to the shareholders. In general, there is a legal obligation to continuously investigate risks and maintain an adequate level of security.

Among the factors affecting the security requirements for a cloud service, importance of the information processed is as well how it needs to be protected (confidentiality, integrity, secure backup etc.), and what availability that is required. To facilitate the assessment of the availability level required, organizations need to analyze their business processes on a high level and also map out which IT resources and information systems etc. that are used in the processes. Following, an assessment of which business processes that are critical, i.e. that always need to be operational or operate at a very high level of availability, should be conducted. It is easier to "cloud source" the support for parts or whole business processes that are not critical. A security audit of a cloud service requires significant time and resources. Thus, an organization ought to be more thorough while auditing cloud services used in critical business processes compared to for non-critical business processes. A security audit should not only be made initially, but be made continuously as long as the cloud service is used. The security audit should always use your own policies related to the

area. Input to the audit requirements are, for example, changes in business and business environment requirements. Consequently, it is a good idea to start with a business process which is non-critical nor processes any confidential information, to learn and get experience before addressing critical business processes where demands are higher. Required are an analysis and a plan.

In addition to listing and highlighting issues and problems, we link what business value can be created upon appropriate planning, management and actions pertaining to those issues or problems.

Concerning business value for an organization, business value can be interpreted very differently, depending on type of organization, its mission and stakeholders. Preferably, the business value should be measured in straight figures like total-cost-of-ownership (TCO), where the cost for having a solution run by the organization is compared to using a cloud service, return-on-investment (ROI) or the like. However, finding these costs and cash flows can be difficult, as many of the business values are qualitative rather than quantitative. We suggest, as part of any cloud services business case, that the business value generated from information security and related topics are described and highlighted – in order to show that not only costs are generated but also business value. Examples of business value categories, found in business literature and research, applicable for a cloud service context are: improved organizational performance/profitability (PERFORMANCE), improved competitive advantage (COMPETITIVENESS), creative synergy (SYNERGY), respectively improved management ability (MANAGEMENT). Below, there are one or more examples of different business values for each category:

- **PERFORMANCE** – productivity increase, more efficient processes, lower costs, increased profitability, higher return on capital or investment, increased sales, more mobile workforce.
- **COMPETITIVENESS** – facilitator for new products or services, improved adaptability/changeability and scalability (i.e. pay for usage), increased ability to attract or get resources that are difficult to imitate/rare/valuable/non-substitutable and make these productive and create competitive advantage, more content customers and employees, shorter time to markets for products/services, lower cost barrier, ability to reach new markets, lowered risk.
- **SYNERGY** – improve the relation between information systems/IT and organization/strategy/ structures/management processes to create synergies among strategies/organization/processes/technology/humans and further increase the effect from technology to reach higher profitability.
- **MANAGEMENT** – management gets better understanding of available resources/customers etc. that may lead to better sourcing of resources and improved product/service design, management and organization are better prepared to manage a crisis, increased trustworthiness/reliability from customers and the own organization, organization is able to manage business/legal requirements.

This document has a focus on improved management ability. Recommended is that you, besides using this document, further read and use the documents listed in the reference section.

## 2. Aspects to consider within information security during procurement and use of cloud services

This section does not comprise a complete collection of areas or problems that need to be considered. The intention is to provide a basic structure for the work regarding security to enhance and continue to build upon. Hopefully this basic structure will enable organizations to save time, resources and money. The sources used are explicitly marked as references. However, the authors' own experiences or research have been added into the text without any explicit references.

The areas/problems are tagged with a level, which corresponds to the level where the area/problem should be addressed. The levels used are strategic (s), tactical (t) and operative (o). By *strategic* we mean top management level consideration and decision that affect a whole organization with a long time frame (i.e. years). By *tactical* we mean the management responsibility for functions or processes and decisions that affect people's work with a medium time frame (i.e. months). Finally, by *operative* we mean department or group level where the decisions impact on the daily business with a short time frame (i.e. weeks or days). Suggested is to start with the strategic level areas and problems, and work downwards to the operative level.

Below is a list of security areas/problems to consider:

| Level | Area/Problem | Who has most interest | Source |
|---|---|---|---|
| S | Compliance[1] with legal requirements and regulations. Which are fulfilled, and which need to be fulfilled? | Top management | [1, 4] |
| S | Compliance with the own security policy. Anything that renders problems? Is there a need to change the own security policy? | Top management | [1, 3, 4, 6] |
| S | Fulfillment of requirements from standards, certify-cations, "best practices" etc. (i.e. compliance). Which requirements should/must we fulfill and - which does the provider fulfill? How can we demonstrate this at a (re)certification? | Top management | [1, 3, 4] |
| S | Audit and evidence collection. How can audits be conducted, and how can potential evidence needed be collected? Is there a common audit for all customers together? | Top management | [3] |
| S | Risk management – transparency at provider. Is it possible to maintain a continuous high qualitative risk management/mitigation? Are there audits made by independent third parties after a standard model with publicly known criteria or metrics? Are the audit protocols for a number of previous years available? | Top management, procurement function | [1, 3, 4] |
| S | Insurance. Does the provider have an insurance which covers damages or costs that can arise due to data breach, mistakes or other causes?<br>Does insurance cover what the identified risks can cause? | Top management, procurement function | |

[1] It can be worth noting that not only Swedish and EU legislation need to be considered, as planned and existing legislation in the USA can have an impact as well.

| | | | |
|---|---|---|---|
| S | Information issues. Will our organization have ensured access to our own information during a certain period of time from a notified point in time, even if the cloud service is shut down for any reason, or during a contractual dispute? Ownership of information – always owned by our own organization no matter what? Will the information be kept partitioned at storage and processing (possible to recreate if one or more partitions fail), and is it due to the partitioning more difficult to recreate information at a breach? Is the information stored or processed globally, or at appointed data centers? The last issue is of importance if there is sensitive personal information which is affected by, for example, the EU Data Protection Directive, and Safe Harbor/Patriot Act in the USA etc. | Top management | [1, 3, 4] |
| S | Long term digital preservation and storage. How do we want this to be set up and operate? Who has responsibility for migration and emulation etc. of the formats stored? Does the provider manage all this, or is more knowledge and competence needed? | Top management, CIO | |
| S | In case of a potential change of cloud service. Is it possible to port (or directly use) the information and its meta-data in new environments and other providers' cloud services? | Top management, CIO, architect | [3, 4] |
| S | Business continuity planning – to extend the own or synchronize with the provider's. Is it easy, or does it comprise a large effort? How often to practice? | Top management, resp. for business continuity planning | [1, 3, 4] |
| S/T | How far does the provider's responsibility stretch and where does the own responsibility end (does the provider responsibility end at the hypervisor, i.e. the virtualization/physical- and environmental security, or does it stretch shorter/longer)? What applies for security checks of infrastructure, operating systems, data/information, applications etc.? Is the virtualization shared with other customers, or is all separated per customer? How do we want it? | Top management, procurement function | [3, 4] |
| S/T | Disaster recovery planning on cloud service/system level – how is it set up? Are our own services/systems integrated with the provider's? | Top management, IT and Information systems departments | [1] |
| S/O | Disaster recovery – how is the provider's process devised? Is there a need to integrate with our own process, or is it enough that the provider's process looks OK? How often to test? | Top management, IT and Information systems departments, operation/support | [3, 4] |
| S/O | Incident response – how is the provider's process set up, and how can the own process be integrated with the provider's process? How often to test? | Top management, IT and Information systems departments, operations/support | [1, 4] |

| | | | |
|---|---|---|---|
| T | Identity and access management (IAM). How many such IAM-systems will our organization be involved in? Are there proprietary and/or different variants used by the potential providers? Some of these IAM-systems require additional knowledge, resources and separate control processes. Is it possible to find an interoperable solution that all or several providers can use in common? How many security levels are required? What users/roles will we need to have? Do we have a process to add/remove users and roles? | Architect, procurement function | [1, 2, 3] |
| T | Service integrity. Does the provider's development process concern security and personal integrity issues during the whole lifecycle of the cloud service? Does the delivery of the cloud service fulfill the contractual requirements on security (availability, monitoring/audit/ logging, response times and support level)? | Procurement function | [1, 3, 4] |
| T | Security at end users (i.e. end point security). Do we need training and an awareness program to achieve a secure behavior (for example, towards social engineering, identity theft, phishing, viruses, malicious links etc.)? How should users (and administrators) securely connect to the cloud service – requirements? Is it possible to have "single sign-on" together with other cloud services/systems depending on how directory services, keys, key management and firewall policies look like? What does the own security policy require of the IT environment and users in general? | CISO | [1, 3, 4] |
| T | Security in the cloud service interfaces. How are the cloud service's security levels in the interfaces set up? Are the interfaces for instance securely developed, see [5], and are any APIs (Application Programming Interfaces) or other possibilities to connect within, around or to the cloud service secure and securely developed? Encryption levels and key generation/management? How and how often is all this tested? | CISO | [2, 3, 4] |
| T | Protection of information. Is the information always protected while being within the cloud service according to the requirement/classification in the security policy (encryption, integrity, backup and recovery etc.)? How is the information kept separated from other organizations' information? Levels of encryption and key management – how are these set up? Backup – method, safe and secure storage? How often is all this tested? | CIO/CISO | [1, 2, 3, 4] |
| T | Dynamics of the cloud service. How quickly can additional resources or performance always be provided, and for how long? What is our need regarding dynamics? | CIO | [3] |

| | | | |
|---|---|---|---|
| O | Physical security, background checks and logging of personnel at the provider etc. The requirements posed on the provider shall mirror the own business requirements on security. Are backups safe and secure? | Buyer | [1, 3] |
| O | Is the cloud service developed to prevent intrusion? In case of an intrusion, will the intruder get access to information stored in other data centers? What is monitored and logged? How is the monitoring function set up, and is it manned 24x7? | Buyer, CISO | [2, 4] |
| O | Does the cloud service have a standardized open interface to MSS (managed security services) providers for its customers? Do we need or want this? | Buyer, CISO | [3] |
| O | Patch management. How is patch management managed within the cloud service software, security solutions and supportive software like operating systems, device drivers, virtualization etc.? Is there a process for this and is it executed in a controlled manner? Are always new parameter settings changed by a patch reverted back to the prior settings if wanted? | Buyer, CISO | [2, 3] |
| O | Who have, and who should have access and be able to log in to the cloud service, supportive software, and the information stored in the cloud service? Do these really need to be able all that they can, or do they have too much access rights or authorization (goes for both employees at the provider and the own organization)? | Buyer, CISO | [2] |
| O | How often are penetration tests and different attacks applied towards the cloud service? What were the results of prior penetration tests? Examples are attacks towards password sources and authentication mechanisms, password- and key cracking, availability (DDOS/EDOS) etc.? | Buyer, CISO | [2, 3] |
| O | Can any user add links, applications or other source code to the cloud service? If needed, can this be controlled by authorization? Logging? | Buyer, CISO | [2] |
| O | Removal/deletion of data. If data should be removed/deleted on demand by us, how is this managed and how can we ensure that the data has really been removed/deleted? How long will it take? What goes for the backups? | Buyer, CISO | [3] |

## 3. Creating a compliance framework for cloud computing – what to address in such a framework?

A compliance framework for cloud computing should preferably be integrated into an organization's overall risk management and compliance set up. Compliance can be seen as a tool for top management to ensure that risks are managed and requirements from legal/regulatory bodies, customers, standards, certifications or best practices that should be honored are in fact honored. Further, if an organization has additional internal requirements that should be upheld, those can be added to a compliance framework as well to be followed up on and kept updated. There are a number of ways to set up an organization's overall risk management and compliance activities, but those will not be covered in this document.

The idea with this section is that an organization should get an idea on what "elements/controls" that a simplistic compliance framework for cloud computing can comprise. The elements/controls are aimed to be input for risk management departments, CIOs, CISOs, or other functions or roles responsible to honor requirements or to proactively monitor, manage and mitigate existing and emerging risks related to cloud services used by the organization in its operations. A further comprehensive set of elements/controls can be found in [7] (which maps to various international standards), and if used it should be adapted to your organization and the applicable Swedish conditions related to your business context.

Below are a number of elements/controls that can be part of a cloud computing compliance framework:

- Risk management – transparency at provider. Needed is to maintain a continuous high qualitative risk management/mitigation. Do we do the audits ourselves, or are the audits made by independent third parties after a standard model with publicly known criteria or metrics? Where are the audit protocols for a number of previous years available? [1, 3, 4]
- Risk management – internal. What risks should be tracked and how often should risk evaluations be conducted? Who is responsible and will manage the risk mitigation?
- Compliance[2] with legal requirements and regulations. Which need to be fulfilled, which are and which remain to be fulfilled? [1, 4]
- Fulfillment of requirements from standards, certifications or "best practices" etc. Which requirements should/must we fulfill and - which does the provider fulfill? If there is a gap – how to manage that gap? How can we demonstrate this at a (re)certification? [1, 3, 4]
- Compliance with essential customer requirements. Which are the essential requirements (necessary to stay in business), and which are fulfilled or remain to be fulfilled?
- Compliance with the own security policy or polices. Anything that renders problems? Is there a need to change the own security policy? [1, 3, 4, 6]
- Business continuity planning – is the business continuity planning involving the provider and our own organization's related critical processes in line with the internal/external requirements (i.e. available within a decided timeframe in case of problems)? How often to practice crisis management, disaster recovery and incident response? [1, 3, 4]

[2] It can be worth noting that not only the Swedish and EU legislation need to be considered, as planned and existing legislation in the USA can have an impact as well.

## 4. Sources


[i] Cloud Sweden (2011). Areas and problems to consider within information security and digital preservation during procurement and use of cloud services, v1.1.1, http://natverk.dfs.se/node/21531#attachments

[1] Microsoft (2010). Cloud Computing Security Considerations. www.microsoft.com
[2] CSA – Cloud Security Alliance (2010). Top Threats to cloud computing v1.0. www.cloudsecurityalliance.org
[3] ENISA (2009). Cloud Computing: Benefits, risks and recommendation for information security. www.enisa.eu
[4] CSA – Cloud Security Alliance (2009). Security Guidance for critical areas of focus in cloud computing v2.1. www.cloudsecurityalliance.org
[5] OWASP (2010). OWASP top ten project - www.owasp.org
[6] Microsoft (2010). Information Security Management System for Microsoft Cloud Infrastructure - http://www.globalfoundationservices.com/security/documents/InformationSecurityMangSysforMSCloudInfrastructure.pdf
[7] CSA – Cloud Security Alliance (2013). Cloud Controls Matrix v1.4 - https://cloudsecurityalliance.org/research/ccm/


Personal information – Swedish Personal Data Act and the Personal Data Ordinance, and the Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

Further documents of interest can found at CSA's main homepage at: https://cloudsecurityalliance.org/